

[| NODIS Library](#) | [Organization and Administration\(1000s\)](#) | [Search](#) |

# NASA Procedural Requirements

**NPR 1600.2**Effective Date: October 11,  
2011Expiration Date: October 11,  
2016**COMPLIANCE IS MANDATORY**[Printable Format \(PDF\)](#)

Request Notification of Change (NASA Only)

## **Subject: NASA Classified National Security Information (CNSI) w/Change 2 (2/12/2014)**

**Responsible Office: Office of Protective Services**[| TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [AppendixA](#) | [AppendixB](#) | [AppendixC](#) | [ALL](#) |

## **Appendix A: Definitions**

**Access.** The ability or opportunity to gain knowledge of classified information.

**Adjudication.** A fair and logical Agency determination, based upon established adjudicative guidelines and sufficient investigative information, as to whether or not an individual's access to classified information, suitability for employment with the U.S. Government, or access to NASA facilities, information, or IT resources, is in the best interest of national security or efficiency of the Government.

**Authorized holder.** Anyone who satisfies the conditions for access to classified information in accordance with section 4.1 (a) in Exec. Order No. 13526.

**Automatic declassification.** The declassification of information based solely upon the occurrence of a specific date or event as determined by the original classification authority or the expiration of a maximum timeframe for duration of classification established under Exec. Order No. 13526 .

**Center Chief of Security (CCPS/CCS).** The senior Center security official responsible for technical management of the Center security program.

**Central Adjudication Facility (CAF).** Facility established at the Security Management Division-level which is responsible for adjudicating all requests for clearances to access CNSI.

**Certification.** A formal process used by the Certifying Official to ensure that an individual has met all established training requirements necessary to perform their security responsibilities.

**Classification.** The act or process by which information is determined to be classified information.

**Classification guidance.** Any instruction or source that prescribes the classification of specific information.

**Classification Guide.** A documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

**Classified Material.** Any physical object on which is recorded or in which is embodied CNSI that must be discerned by the study, analysis, observation, or other use of the object itself.

**Classified National Security Information (CNSI).** Information that must be protected against unauthorized disclosure in accordance with Exec. Order No. 13526, "Classified National Security Information," as amended and is marked to indicate its classified status when in documentary form.

**Closed Area.** An area in which security measures are taken to safeguard classified material where entry to the area alone provides visible or audible access to classified material.

**Collateral Classified.** All CNSI, excluding information in the SCI or SAP information category.

Communications Security (COMSEC). Measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes crypto security, transmission security, emission security, and physical security of COMSEC material.

Compilation. An aggregation of preexisting unclassified items of information.

Compromise. The improper or unauthorized disclosure of or access to classified information.

Contractor. For the purpose of this NPR, any non-NASA entity or individual working on a NASA installation or accessing NASA information technology.

Damage. Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

Declassification. The authorized change in the status of information from classified information to unclassified information.

Declassification Guide. Written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

Declassification Authority (DCA). An official delegated declassification authority in writing by the Agency head or the SAO.

Denial. The adjudication that an individual's initial access to classified information would pose a risk to national security, after review procedures set forth in Exec. Order No. 13526 have been exercised.

Derivative classification. The incorporation, paraphrasing, restating, or generation of a new form of information that is already classified and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

Document. Any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

Downgrading. A determination by a declassification authority that information classified and safeguarded at a specified level must be classified and safeguarded at a lower level.

Escort. A NASA civil service employee or contractor responsible for the management of a visitor's movements and/or accesses implemented through the constant presence and monitoring of the visitor by appropriately designated and properly trained U.S. Government or approved contractor personnel. Training includes the purpose of the visit, where the individual may access the Center, where the individual may go, whom the individual is to meet, and authorized topics of discussion.

File Series. File units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

Foreign Government Information. (1) Information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence. (2) Information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, an international organization of governments or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence. (3) Information received and treated as foreign government information under the terms of a predecessor order.

Foreign National. For the purpose of general security protection, considerations of national security, and access accountability: Any person who is not a citizen of the United States. Includes lawful permanent resident (i.e., holders of green cards) or persons admitted with refugee asylee status to the United States.

Formerly Restricted Data (FRD). Defined by the Atomic Energy Act as classified information which has been removed from the RD category after DOE and the DOD have jointly determined that it relates primarily to the military's utilization of atomic weapons and can be adequately safeguarded as national security information.

Information Security Oversight Office (ISOO). Office established under the Executive Office of the President tasked with policy development and oversight of Federal agency compliance with national-level policy for management of CNSI.

Intergovernmental Personnel Act (IPA). Individuals on temporary assignments between Federal agencies and state,

local, and Indian tribal governments, institutions of higher education, and other eligible organizations. IPAs can include foreign nationals.

**Limited Area.** An area in which security measures are taken to safeguard classified material or unclassified property warranting special protection. To prevent unauthorized access to such property, visitors must be escorted or other internal restrictions implemented, as determined by the CCPS/CCS.

**Mandatory Declassification Review.** The review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of Exec. Order No. 13526.

**NASA Employee.** NASA civil service personnel.

**National Security.** The national defense or foreign relations of the United States.

**National Security Position.** Positions that have the potential to cause damage to the national security. These positions require access to classified information and are designated by the level of potential damage to the national security:

**Confidential.** Information, the unauthorized disclosure of which reasonably could be expected to cause damage to national security that the Original Classification Authority is able to identify or describe.

**Secret.** Information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to national security that the Original Classification Authority is able to identify or describe.

**Top Secret.** Information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security that the OCA is able to identify or describe.

**Need-to-Know.** A determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

**Nondisclosure Agreement.** Standard Form 312 (SF 312) is a non-disclosure agreement required under Exec. Order No. 13292 to be signed by employees of the U.S. Federal Government or one of its contractors when they are granted a security clearance for access to classified information. The form is issued by the ISOO of the NARA and its title is "Classified Information Nondisclosure Agreement." SF 312 prohibits confirming or repeating classified information to unauthorized individuals, even if that information is already leaked. The SF 312 replaces the earlier forms SF 189 or the SF 189-A. Enforcement of SF 312 is limited to civil actions to enjoin disclosure or seek monetary damages and administrative sanctions, "including reprimand, suspension, demotion, or removal, in addition to the likely loss of the security clearance."

**Original Classification.** An initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

**Original Classification Authority (OCA).** An individual authorized in writing, either by the President, by agency heads, or other senior Government officials designated by the President, to classify information in the first instance.

**Page Check.** Involves visually sighting each page in a document, verifying its presence against a list of effective pages (if applicable), and ensuring that the page is from the original document. In the absence of a list of effective pages, the document will be examined for continuity.

**Permanent Resident Alien.** A non-U.S. citizen legally permitted to reside and work within the United States and issued the Resident Alien Identification (Green Card). Afforded all the rights and privileges of a U.S. citizen with the exception of voting, holding public office, employment in the Federal sector (except for specific needs or under temporary appointments per 3 C.F.R. Part 7, Section 7.4), and access to CNSI. Permanent Resident Aliens are not prohibited from accessing export controlled commodities, but must still have a work-related need-to-know and are still considered foreign nationals under immigration laws.

**Records.** The records of an agency and Presidential papers or records, as those terms are defined in 44 U.S.C. § 2905, § 3101, and § 3102, including those created or maintained by a Government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant. Records having permanent historical value include Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with 44 U.S.C. § 2905, § 3101, and § 3102.

**Restricted Area.** An area in which security measures are taken to safeguard and control access to property and hazardous materials or to protect operations that are vital to the accomplishment of the mission assigned to a Center or Component Facility. All facilities designated as critical infrastructure or key resource must be "Restricted" areas (as a minimum designation).

**Restricted Data (RD).** Defined by the Atomic Energy Act as all data concerning design, manufacture, or utilization of atomic weapons, production of special nuclear material, and use of Special Nuclear Material in the production of

energy.

Safeguarding. Measures and controls that are prescribed to protect classified information.

Security Classification Guide. The written direction issued or approved by a Top Secret/OCA that identifies the information or material to be protected from unauthorized disclosure and specifies the level and duration of classification assigned or assignable to such information or material.

Security Clearance. A designation identifying an individual's highest level of allowable access to classified information based upon a positive adjudication that the individual does not pose a risk to national security.

Security Management Division Director. Official assigned to the OPS who is responsible for Agency management of physical security, industrial security, program security, and NASA Federal Arrest Authority and Certification.

Self-inspection. The internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under Exec. Order No. 13526 and its implementing directives.

Senior Agency Official (SAO). The official designated by the agency head under section 5.4 (d) of Exec. Order No. 13526 to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

Sensitive Compartmented Information (SCI). Classification level denoting information, generally intelligence related, requiring security clearances and physical/procedural security measures above those established for collateral classified information or SAP information.

Source Document. An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

Special Access Program (SAP). Any program established and approved under Exec. Order No. 13526 that imposes need-to-know or access controls beyond those normally required for access to collateral Confidential, Secret, or Top Secret information.

Suspension. The temporary removal of an individual's access to classified information, pending the completion of an investigation and final adjudication.

Systematic Declassification Review. The review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value in accordance with 44 U.S.C. § 2905, § 3101, and § 3102.

Unauthorized Disclosure (Exec. Order No. 13526). A communication or physical transfer of classified information to a recipient who does not have the appropriate credentials for access.

Waiver. The approved continuance of a condition authorized by the AA for Protective Services that varies from a requirement and implements risk management on the designated vulnerability.

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [AppendixA](#) | [AppendixB](#) | [AppendixC](#) | [ALL](#) |

| [NODIS Library](#) | [Organization and Administration\(1000s\)](#) | [Search](#) |

## **DISTRIBUTION:** **NODIS**

---

### **This Document Is Uncontrolled When Printed.**

Check the NASA Online Directives Information System (NODIS) Library  
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>

---